U.S. Department of Justice

United States Attorney
District of New Jersey

970 Broad Street, Suite 700 *(973) 645-2728*
Newark, NJ 07102 *Facsimile (973) 645-2857*

Michael Martinez
Executive Assistant United States Attorney
Zach Intrater
Assistant United States Attorney

March 13, 2013

Honorable Susan D. Wigenton
United States District Judge
Martin Luther King Jr. Federal Courthouse
50 Walnut Street
Newark, New Jersey 07102

Re: United States v. Andrew Auernheimer, No. 11-470 (SDW)

Dear Judge Wigenton:

Please accept this letter brief in lieu of a more formal submission. It summarizes the United States's position on the appropriate sentence for defendant Andrew Auernheimer.

The defendant is a well-known computer hacker and internet "troll." For years, he has engaged in a series of increasingly serious computer intrusions, attacks, and exploits, exclusively in the interest of building his reputation in the hacking world, and of profiting through his notoriety.

In November 2012, the defendant's chosen "career" of wreaking havoc on the Internet caught up with him. A jury convicted defendant Auernheimer on both counts of a two-count Superseding Indictment. The evidence at trial proved that his was a case of theft by deception: In June 2010, defendant Auernheimer and his co-conspirator, working as part of a group of so-called "security researchers" who called themselves "Goatse Security," created a piece of computer code. The computer code pretended to be Apple iPads – in fact, it pretended to be more than 114,000 different, unique iPads, including over 4,000 iPads belonging to victims residing in New Jersey.

The defendant and his co-conspirator used this computer code to lie to computer servers belonging to AT&T and steal the personal identifying information of more than 114,000 iPad users. The stolen information consisted of the personal e-mail addresses and Integrated Circuit Card Identifiers ("ICC-IDs") for users of the iPad, a tablet computer. Only by deceiving, by lying, and by tricking, did the defendant and his co-conspirator get those users' information.

Then, defendant Auernheimer took these iPad users' personal information – without obtaining permission from a single, solitary user – and disclosed that personal information to a reporter from the website Gawker.

Defendant Auernheimer committed this theft and unlawful disclosure so that he could publicize his computer security research firm and market it to businesses that were worried about cyber-thefts, like the one the defendant committed here. In short, defendant Auernheimer was motivated by publicity and greed – he thought that because he and his cohorts were skilled computer hackers, they could violate peoples' privacy, and get famous doing it.

And this was of a piece with defendant Auernheimer's history. His entire adult life has been dedicated to taking advantage of others, using his computer expertise to violate others' privacy, to embarrass others, to build his reputation on the backs of those less skilled than he.

But the defendant maintains he has done nothing wrong. And this is a critical reason why the defendant must be punished for his crimes. Rather than accept personal responsibility or his criminal conduct and start down the path toward rehabilitation, the defendant consistently paints himself as the victim of a government and corporate conspiracy. If left unpunished, the defendant will – by his own admission – continue to engage in computer intrusions; continue to access computers without authorization; and continue to draw attention to himself through damaging exploits in the cyber world. And so specific deterrence is a primary reason why the defendant deserves a sentence of imprisonment within the Guidelines range.

General deterrence is equally important. It is a truism that with each passing year, we spend more of our lives online. Defendant Auernheimer and his co-conspirator belong to a class of people with sophisticated computer skills. Unlike many of us, they understand how to extract valuable information belonging to other people from computer servers. A Guidelines sentence will help deter those individuals from using their sophisticated computer skills to violate the privacy rights of innocent others.

Therefore, to account for the seriousness of the offense and the history and characteristics of defendant Auernheimer, to afford adequate deterrence to criminal conduct, and to protect the public from further crimes of defendant Auernheimer, the Court should impose a sentence within the advisory Guidelines range.

After *United States v. Booker*, 543 U.S. 220 (2005), sentencing involves a three-step process: "(1) Courts must continue to calculate a defendant's Guidelines sentence precisely as they would have before *Booker*. (2) ... [courts] must formally rule on the [departure] motions of both parties and state on the record whether they are granting a departure and how that departure affects the Guidelines calculation .... (3) Finally, [courts] are required to exercise their discretion

by considering the relevant [18 U.S.C.] § 3553(a) factors in setting the sentence they impose ...." *United States v. Ali*, 508 F.3d 136, 142 (3d Cir. 2007). The Government respectfully submits that this sentencing analysis should result in a sentence within the advisory Guidelines range.

I. The Guidelines Range

The United States Probation Office has calculated defendant Auernheimer's advisory Guidelines range to be a level 20. *See* P.S.R. at ¶ 72. Defendant Auernheimer's base offense level is 6. *See* U.S.S.G. § 2B1.1(a)(2). Defendant Auernheimer's crimes caused an actual loss of approximately $73,000 suffered by AT&T; this results in an increase of 8 levels. *See id.* at § 2B1.1(b)(1)(E). Defendant Auernheimer's crimes caused the dissemination of personal information; this results in an increase of 2 levels. *See id.* at § 2B1.1(b)(16). Defendant Auernheimer and his co-conspirator used sophisticated means to commit their offenses; this results in an increase of 2 levels. *See id.* at § 2B1.1(b)(10)(C). Finally, defendant Auernheimer and his co-conspirator utilized special skills – their computer skills – to commit their crimes; this results in an increase of 2 levels. *See id.* at § 3B1.3.

Combined with a criminal history category of I, defendant Auernheimer's Guidelines range is 33-41 months' imprisonment.

Defendant Auernheimer will likely make an argument challenging the loss figure as calculated by the Probation Department. This argument should fail by the black letter terms of the Guidelines. Application Note 3 of U.S.S.G. § 2B1.1 "applies to the determination of loss under subsection [§ 2B1.1]." The "General Rule" is that "loss is the greater of actual loss or intended loss." *Id.* at Application Note 3(A). In turn, "'[a]ctual loss' means the reasonably foreseeable pecuniary harm that resulted from the offense." *Id.* at Application Note 3(A)(I). The Application Note goes on to state that "'reasonably foreseeable pecuniary harm' means pecuniary harm that the defendant knew or, under the circumstances, reasonably should have known, was a potential result of the offense." *Id.* at Application Note 3(A)(iv). Finally, the Guidelines contain an explicit reference to 18 U.S.C. § 1030: "In the case of an offense under 18 U.S.C. § 1030, actual loss includes the following pecuniary harm, regardless of whether such pecuniary harm was reasonably foreseeable: any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other damages incurred because of interruption of service." *Id.* at Application Note 3.(A)(v)(III).

II. Departures

The Government does not believe that any departures are warranted; it does not move here for any departures from the advisory Guidelines sentencing range of 33-41 months'

imprisonment. Because the parties are filing their sentencing memoranda simultaneously, the Government does not know whether defendant Auernheimer will be moving for a departure from the applicable Guidelines range. If defendant Auernheimer makes any such motion, however, the Government respectfully requests the opportunity to be heard before this Court imposes sentence.

III. Application of the Section 3553(a) Factors

The Court must give "'rational and meaningful consideration [to] the factors enumerated in 18 U.S.C. § 3553(a)'" and make an "'individualized assessment based on the facts presented.'" *United States v. Tomko*, 562 F.3d 558, 567 (3d Cir. 2009) (en banc). Under § 3553(a), "[t]he Court shall impose a sentence sufficient, but not greater than necessary, to comply with the purposes" of sentencing. 18 U.S.C. § 3553(a). Those purposes are "(A) to reflect the seriousness of the offense, to promote respect for the law, and to provide just punishment for the offense; (B) to afford adequate deterrence to criminal conduct; (C) to protect the public from further crimes of the defendant; and (D) to provide the defendant with needed educational or vocational training, medical care, or other correctional treatment in the most effective manner." 18 U.S.C. § 3553(a)(2).

In determining that sentence, this Court must consider "the nature and circumstances of the offense and the history and characteristics of the defendant," 18 U.S.C. § 3553(a)(1), "the kinds of sentences available," § 3553(a)(3), the Guidelines and Guidelines range, § 3553(a)(4), the Guidelines' policy statements, § 3553(a)(5), "the need to avoid unwarranted sentence disparities among defendants with similar records who have been found guilty of similar conduct," § 3553(a)(6), and "the need to provide restitution to any victims of the offense," § 3553(a)(7). Of course, a "sentencing court does not enjoy the benefit of a legal presumption that the Guidelines sentence should apply," *Rita v. United States*, 127 S. Ct. 2456, 2465 (2007), and "may not presume that the Guidelines range is reasonable," *Gall v. United States*, 552 U.S. 38, 128 S. Ct. 586, 596-97 (2007); *Nelson v. United States*, 129 S. Ct. 890, 892 (2009).[1]

What follows is an explanation of why the § 3553(a) factors support a sentence within the Guidelines range in this case.

---

[1] Giving such "presumptive weight" to the Guidelines is error. *United States v. Hawes*, 523 F.3d 245, 256 (3d Cir. 2008).

A. Nature and Circumstances/Seriousness of the Offense

The iPad, introduced to the market in January 2010, was a device developed and marketed by Apple Computer, Inc. It was a touch-screen tablet computer, roughly the size of a magazine. The iPad allowed users to, among other things, access the Internet, send and receive electronic mail, view photographs and videos, read electronic books, word-process, and create spreadsheets and charts.

AT&T Communications, Inc. ("AT&T") provided certain iPad users with Internet connectivity via AT&T's 3G wireless network.[2] Apple iPad 3G users who wished to subscribe to the AT&T 3G network had to register with AT&T. During the registration process, the user was required to provide, among other things, an e-mail address, billing address, and password.

At the time of registration, AT&T automatically linked the iPad 3G user's e-mail address to the Integrated Circuit Card Identifier ("ICC-ID") of the user's iPad, which was a 19 to 20 digit number unique to every iPad. Accordingly, each time a user accessed the AT&T website, his ICC-ID was recognized and, in turn, his e-mail address was automatically populated, providing the user with speedier and more user-friendly access to the website. The ICC-IDs and associated iPad 3G user e-mail addresses were not available to the public and were kept confidential by AT&T.

Prior to mid-June 2010, when an iPad 3G communicated with AT&T's website, its ICC-ID was automatically displayed in the Universal Resource Locator, or "URL," of the AT&T website in plain text. Seeing this, and discovering that each ICC-ID was connected to an iPad 3G user e-mail address, the co-conspirators wrote a script termed the "iPad 3G Account Slurper" (the "Account Slurper") and deployed it against AT&T's servers. AT&T's servers were protected computers as defined in Title 18, United States Code, Section 1030(e)(2).

The Account Slurper attacked AT&T's servers for several days in early June 2010, and was designed to harvest as many ICC-ID/e-mail address pairings as possible. It worked as follows: the Account Slurper was designed to mimic the behavior of an iPad 3G so that AT&T's servers were fooled into believing that they were communicating with an actual iPad 3G and wrongly granted the Account Slurper access to AT&T's servers. Once deployed, the Account Slurper utilized a process known as a "brute force" attack – an iterative process used to obtain information from a computer system – against AT&T's servers. Specifically, the Account

[2] Both Wi-Fi and the 3G wireless network were mechanisms by which users could access the Internet. For some iPad models, Internet connectivity was provided strictly over Wi-Fi, while others offered a combination of Wi-Fi and AT&T's 3G wireless network.

Slurper guessed at ranges of ICC-IDs. An incorrect guess was met with no additional information, while a correct guess was rewarded with an ICC-ID/e-mail pairing for a specific, identifiable iPad 3G user.

During its attack on AT&T's servers, the Account Slurper gained unauthorized access to AT&T's servers, and ultimately stole for the co-conspirators more than 114,000 ICC-ID/e-mail address pairings for iPad 3G customers. This was done without the authorization of AT&T, Apple, or any of the individual iPad 3G users.

Goatse Security members communicated with one another in what are essentially chat rooms, which are known as Internet Relay Chat ("IRC") channels. Before, during, and after the theft, the Goatse Security members discussed the scheme – in great detail – over IRC. These chats provided devastating evidence of the nature and circumstances of the offense – what defendant Auernheimer and his cohorts were thinking in real time as they committed their offenses.

What did defendant Auernheimer do with the personal information of over 114,000 iPad users? Defendant Auernheimer publicized the theft. He pored through the list of stolen information, looking for domain names that seemed connected to the media. *See* 11/14/12 Tr. at 81:6-8 ("Q: Did the defendant ask you for e-mail addresses for people in any particular industry? A: Yeah, the news media.") Then, defendant Auernheimer sent e-mails to several of these media-connected victims. These users included a board member at the News Corporation, the general counsel of the Washington Post Company, and reporters at Reuters.

In the e-mails, defendant Auernheimer stated that he "stole" the victims' e-mails and ICC-IDs, and stated that if the victims contacted him, he "would be absolutely happy to describe the method of theft in more detail." *See* 11/15/12 Tr. at 33:9-10. Those were his words, at the time of the breach. He knew, at the very moments he was composing his e-mails, that his access was unauthorized; that he was stealing from AT&T and stealing from the iPad users.

Defendant Auernheimer then sent the stolen information to a reporter at Gawker, a popular news/gossip website, along with an e-mail describing exactly what Goatse Security had done. When defendant Auernheimer sent the list to the reporter at Gawker, he sent the entire list. He did nothing to redact any information from the list. And again, as Spitler testified, the way in which defendant Auernheimer sent the list was, potentially, completely insecure. Another hacker could have intercepted the list and sold it. Defendant Auernheimer, not AT&T, put the victims at risk. Because defendant Auernheimer did not, does not, care about the security of iPad users. He does not care about the First Amendment. He cares about defendant Auernheimer. As he admitted on cross-examination, "[c]omment and criticism doesn't pay bills." *See* 11/15/12 Tr. at 54:15-16.

Putting all the excuses and bluster aside, defendant Auernheimer discussed, at the very time he was committing the crime, at length and unguardedly, his true motives. Defendant Auernheimer's own words, from the time of the offense, reveal that he wanted to raise the profile of his "security research" group, Goatse Security. And even more importantly, defendant Auernheimer wanted to raise his own profile.

The evidence at trial – including emails, internet chats, and websites that captured the defendant's words while he was committing this crime – proved that the defendant knew he was stealing. Defendant Auernheimer admitted, in emails he sent to employees of the news media at the Washington Post, the San Francisco Chronicle, News Corp, and Thomson Reuters, that he stole their email addresses. Defendant Auernheimer admitted in those same emails to the news media that he also stole the unique identifiers associated with their email addresses. And defendant Auernheimer admitted in those same emails to the news media that he would be absolutely happy to describe his method of theft in more detail.

The evidence at trial also included defendant's private conversations from IRC chat rooms at the very time the defendant and his cohorts were stealing the information. Unbeknownst to the defendant, his words were being contemporaneously recorded by a government informant. In those private conversations, defendant Auernheimer admitted that the services of his computer security research firm were for sale to any corporation or criminal organization that would "write a check of sufficient size." Defendant Auernheimer also admitted, after the news media exploded with articles about his firm's theft, that he intended to capitalize on his firm's newfound publicity by aggressively marketing his firm's services to CEOs.

And it should also be clear what defendant Auernheimer did not do. He did not – ever – contact AT&T and tell them about the breach. *See* 11/15/12 Tr. at 16:8-10 ("I don't want to come to [AT&T]. They can have everything transparent in the press or we cannot have a dialogue.") Defendant Auernheimer lied repeatedly, to various people, about this important fact. He even lied to his co-defendant, Spitler, who believed that defendant Auernheimer had informed AT&T, because defendant Auernheimer told Spitler that defendant Auernheimer would inform AT&T. But he did not. *See* 11/14/12 Tr. at 95:19-25 ("Q: . . . did you have any conversations with the defendant about whether or not he was going to contact AT&T? A: Yes. Q: What did defendant tell you? A: That he was going to contact AT&T. Q: Did he do that? A: No."). In fact, AT&T first learned about the breach from the Washington Post.

When the FBI came to the defendant's home, and executed a search warrant, the defendant tried to destroy evidence. With FBI agents in his residence, the defendant attempted to erase the contents of his computer, but was stopped by the FBI. When FBI agents asked the

defendant why he attempted to erase the contents of his computer, the defendant confessed that the logs on his computer were incriminating.

The defendant's motives were clear. He placed his own interests above those of the more than 114,000 victims. He disclosed their confidential information so that he could generate publicity for himself and his computer security research firm. If his motive had to been to protect the public from corporate security vulnerabilities, then why not send an email to AT&T explaining the vulnerability and providing a small sample of confidential information as corroborative proof? Defendant Auernheimer did not do that because defendant Auernheimer would not have profited – through an enhanced reputation or enhanced business opportunities – if he had quietly disclosed the flaw to AT&T. Accordingly, the nature and circumstances of the offense call for a sentence within the advisory Guidelines range.

B. History and Characteristics of the Defendant

Defendant Auernheimer's actions in this case are of a piece with his personal history. He is a self-professed Internet "troll." A "troll" is a person who intentionally, and without authorization, disrupts services and content on the Internet. Indeed, defendant Auernheimer has previously been public and outspoken about his trolling activities.

For example, in an August 3, 2008 interview with *The New York Times*, defendant Auernheimer admitted: "I hack, I ruin, I make piles of money. I make people afraid for their lives. Trolling is basically Internet eugenics. I want everyone off the Internet. Bloggers are filth. They need to be destroyed. Blogging gives the illusion of participation to a bunch of retards. . . . We need to put these people in the oven!" Likewise, in an interview with the website Corrupt in August 2008, defendant Auernheimer stated: "The security industry does not work against hackers. Security is a myth, there is no system that cannot be broken. . . . For the companies I've targeted, I've showed up at their parties and given some friendly greetings to bask in the looks of disgust and disdain. I take credit and responsibility for my actions." Defendant Auernheimer also maintained a webpage at www.blip.tv, which is a website that, like YouTube, allows users to create and post videos. On his blip.tv page, Auernheimer posted several "sermons" in the guise of the "iProphet." One such video was entitled "Sermon on Fear and The Men In Black/Direct Democracy." During this video, Auernheimer stated: "Trolling can frequently have large economic repercussions as, as I learned, I learned when I trolled Amazon. I saw a one billion dollar change in their market capitalization. That's the most monetary affection [sic] of a publicly traded stock that I've ever personally done. I mean, I've caused a more dramatic shift in price, but never market capitalization." Auernheimer continued: "So a billion dollars changed hands as a result of my trolling, and I'm very, very glad to know that such insignificant things on the Internet can have drastic, far reaching effects."

What did defendant Auernheimer really think about Internet security? Look again to his own words. In March 2010, defendant Auernheimer sought to publicize another of Goatse Security's computer "exploits." (Gov't Ex. 5036, attached as **Exhibit A**.) He wrote an e-mail to an individual running a website called "Encyclopedia Dramatica." The e-mail explained the exploit, and at the end of this e-mail, defendant Auernheimer wrote "About Goatse Security." And he wrote, "We are people that do shit. You may not like what we do, but we get shit done. . . . At Goatse Security, we don't really care about fighting cyberterrorism, or cyber crime, or whatever. We are pioneering new classes of exploits, new methods of evading IDS, and new ways to use computers as tools to make shit happen. Our minds won't be owned by some liar's system of ethics, but they are for rent to any God or Government or corporation or criminal organization that will write a check of sufficient size. We invite you to stop pretending you care about making things more secure and just admit that you're too unskilled to be a real mercenary." (*Id.*) This e-mail, sent while defendant Auernheimer was a member of Goatse Security, while he was engaged in Goatse Security's business, demonstrates exactly what his motives were, and how he saw his role – comment and criticism? Not so much.

But defendant Auernheimer's attitudes towards others on the Internet also had more immediate, more personal, effects on individuals. On December 1, 2009, an individual with the initials M.G. wrote defendant Auernheimer an e-mail. (Gov't Ex. 5015, attached as **Exhibit B**.) M.G. stated that M.G. had discovered an Encyclopedia Dramatica page about M.G., and M.G. begged defendant Auernheimer to take the page down. M.G. wrote, "The things on there are not only hurtful, untrue and cruel but they have caused me to lose my job, my father found it and is furious and I have gone into a deep depression." (*Id.* at 1.) There is no record of defendant Auernheimer's reply to M.G.'s December 1, 2009 e-mail. On December 4, 2009, M.G. wrote defendant Auernheimer another, even more plaintive, e-mail. It stated, "That site is an embarrassment and slander. I am pleading and asking nicely to please have it taken down. If you don't want to could you at least take down the nude photos? I have already gotten fired once cause of it. You've had your fun and made your point, you made me the butt of your jokes, just like it was done in middle school. I'm obviously just a terrible person who deserves nothing but pain and suffering. Please, hasn't it been enough?" (*Id.*)

Defendant Auernheimer's response to the December 4, 2009 e-mail was terse and to the point. He wrote, simply, "$500." (*Id.*)

M.G. then wrote back, asking, "are you saying it will cost $500 to take the page down? I don't have that kind of money. May I ask you, how would you feel if someone made a page about you and your friends and family saw it? Do you know me at all? Do you know anything about me? Why does a human being deserve this?" (*Id.*) Auernheimer responded to this e-mail as well, and again his response was short. He wrote, "[Y]ou're a sex worker, go come up with the money." (*Id.*)

So defendant Auernheimer has a long history of putting his own interests above those whose privacy he chooses to violate on the Internet – that is an essential part of his character. It shows his character. And his actions in the instant case demonstrate that character just as well.

For example, defendant Auernheimer claims that he did not notify AT&T of the security vulnerability because his "motivation was to criticize AT&T." (Tr. 11/15/12 at 50:15). But defendant Auernheimer's actions from the time of the breach reveal his true motive. Defendant Auernheimer was interested in his own reputation, and the reputation of his co-conspirators at Goatse Security.

C. Deterrence and Recidivism

This Court must also consider "the need for the sentence imposed . . . to afford adequate deterrence to criminal conduct" and "to protect the public from further crimes of the defendant[.]" 18 U.S.C. § 3553(a)(2)(B)&(C). The defendant violated the privacy rights of more than 114,000 innocent victims, stealing their confidential, personal identifying information and disclosing it to the press. He committed this theft and unlawful disclosure so that he could publicize his computer security research firm and market it to businesses in need of cyber security. In an attempt to generate newfound publicity for himself and his firm, the defendant sent emails to employees at the Washington Post, the San Francisco Chronicle, News Corp, and Thomson Reuters, boasting about his firm's theft and offering to describe the method of theft in more detail. (Gov't Exs. 5049, 5050, 5052, 5054, attached as **Exhibits C**, **D**, **E**, and **F**.) Moreover, the defendant's firm's website immediately took public credit for compromising AT&T's cyber security and exposing more than 100,000 iPad users. (Gov't Ex. 1003, attached as **Exhibit G**.) And, as the defendant hoped, the news media exploded with articles about his firm's theft. (*See* Tr. 11/13/12 at 32:25-33:11; Gov't Ex. 1000.) The defendant confessed in an IRC chat that he intended to capitalize on his firm's newfound publicity for cyber exploits by aggressively marketing his services to CEOs. (Gov't Ex. 6025, attached as **Exhibit H**.)

The defendant's criminal conduct warrants a sentence of imprisonment within the Guidelines range. Daily life in today's society – from paying bills to dating – is increasingly lived online. And a necessary condition for this societal transformation is that reasonable expectations of privacy are protected in the cyber world as in the physical world. If the defendant does not receive a significant term of incarceration, then other individuals with sophisticated computer skills will be less deterred from criminally exploiting the privacy rights of innocent others for their own professional and financial advancement.

Turning to the need for the sentence "to protect the public from further crimes of the defendant," this factor also demands a Guidelines sentence. When the defendant committed his crimes, he was fully aware that his conduct was illegal. (*See* Gov't Exs. 5049 (describing the co-

conspirators' conduct as theft), 5050 (same), 5052 (same), 5054 (same), 6005 (describing the co-conspirators' conduct as stealing)). Nevertheless, since his arrest, the defendant has engaged in a smear campaign to assign blame for his criminal predicament on others – corporate America, federal prosecutors, FBI agents, and even this Court – rather than accept personal responsibility for his own criminal misconduct and express remorse for the thousands of victims of his crimes.

Sadly, the defendant has refused to take the first step forward in the rehabilitation process: acknowledging his criminal wrongdoing. To the contrary, he has taken several steps backward, casting himself as the victim and foisting blame on others. First, in a statement of responsibility that the defendant published on the Techcrunch website after his conviction, the defendant wrote: "I thought it was egregiously negligent for AT&T to be publishing a complete target list of iPad 3G owners . . . ." (**Exhibit I** at 1.) But, as proven at trial, AT&T published no such list. (*See* Tr. 11/14/12 at 25:14-17, 71:10-24; Tr. 11/15/12 at 74:2-22; Tr. 11/19/12 at 59:24-61:7.) Indeed, the trial evidence established that the defendant and his co-conspirator, Spitler, went to great lengths to write a software program that deceived AT&T's servers into disclosing the confidential, personally identifying information of more than 114,000 iPad users. (*See* Tr. 11/14/12 at 67:3-71:9, 74:22-77:18.) Second, in the same "statement of responsibility," the defendant blamed federal prosecutors and federal agents for wishing him "utterly destroyed." (**Exhibit I** at 2.) He wrote: "This is a country where if you express ideas that federal agents don't like you [sic], you will be beaten, imprisoned, or killed. I accept my responsibility for offending seditious thugs, liars, and tyrants." (*Id.*)

Of course, the defendant's prosecution had nothing to do with the defendant's ideas – e.g., his views regarding corporate America, the federal government, racial equality, or sexual orientation. Rather, the defendant's prosecution was based on his criminal conduct – i.e., accessing a computer without authorization, obtaining the personal identifying information of more than 114,000 individuals, and knowingly possessing, disclosing, and transferring that confidential information. Third, in a Gawker article published shortly after his conviction, the defendant unfairly attempted to undermine the impartiality and integrity of the judiciary, disparaging this Court as "a mean bitch" and stating: "I can see it in her eyes, she's a black Baptist Bush appointee and I don't think she's a fan of the GNAA" – an organization of which the defendant was president. (**Exhibit J** at 5.) Finally, the defendant told the U.S. Probation Office: "I have no contrition. I don't think that I did anything wrong and I don't regret what I did." PSR ¶ 79. In sum, these statements reflect the defendant's conscious and deliberate avoidance of responsibility for his criminal conduct, and augur an atypical recalcitrance by the defendant to conform to the laws regarding unauthorized computer access and the transfer of stolen means of identification. As a result, the need "to protect the public from further crimes of the defendant" requires a sentence within the Guidelines range.

D. The Advisory Guidelines Range

The advisory Guidelines range should be given considerable weight. *United States v. Lloyd*, 469 F.3d 319, 322-24 (3d Cir. 2006) (it is "entirely consistent" with post-*Booker* precedent "for the District Court to give the Guidelines "'great weight'"); *see United States v. Russell*, 564 F.3d 200, 205 (3d Cir. 2009) (no error if, "on most occasions, the District Court agrees that the advisory range provides the appropriate sentence"); *United States v. Ausburn*, 502 F.3d 313, 326 (3d Cir. 2007) ("the advisory range continues to hold significant sway in most cases even after *Booker*"). There are numerous reasons for giving the Guidelines range considerable weight.

First, the Guidelines range is itself a § 3553(a) factor. "The fact that § 3553(a)[(4)] explicitly directs sentencing courts to consider the Guidelines supports the premise that district courts must begin their analysis with the Guidelines and remain cognizant of them throughout the sentencing process." *Gall*, 128 S. Ct. at 597 n.6; *United States v. Langford*, 516 F.3d 205, 211-12, 214 (3d Cir. 2008) (the Guidelines range is the "natural" and "critical" "starting point for the entirety of the § 3553(a) analysis"). Indeed, "the sentencing court must first calculate the Guidelines range, and then consider what sentence is appropriate for the individual defendant in light of the statutory sentencing factors, 18 U.S.C. § 3553(a), explaining any variance from the [Guidelines range] with reference to the latter." *Nelson*, 129 S. Ct. at 891-92.

Second, one of the Sentencing Commission's purposes in promulgating the Guidelines was to "assure the meeting of the purposes of sentencing as set forth in section 3553(a)(2)." 28 U.S.C. §§ 991(b)(1)(A), 994(f). The Commission wrote the Guidelines to "carry out these same § 3553(a) objectives," resulting in "a set of Guidelines that seek to embody the § 3553(a) considerations, both in principle and in practice." *Rita v. United States*, 551 U.S. 338, 127 S. Ct. 2456, 2463-64 (2007); *United States v. Cooper*, 437 F.3d 324, 331 (3d Cir. 2006).

Third, "[t]he federal sentencing guidelines represent the collective determination of three governmental bodies--Congress, the Judiciary, and the Sentencing Commission--as to the appropriate punishments for a wide range of criminal conduct." *Cooper*, 437 F.3d at 331 n.10. Congress is the ultimate maker of sentencing policy, *Mistretta v. United States*, 488 U.S. 361, 363 (1989); *Dorszynski v. United States*, 418 U.S. 424 (1974); *United States v. Wiltberger*, 18 U.S. (5 Wheat.) 76, 94 (1820), and the Guidelines reflect the views of Congress through its instructions to the Commission, the Commission's effort to "establish a sentencing range that is consistent with all pertinent provisions of Title 18," Congress's review of all Guidelines before they take effect, and Congress's direct input into certain Guidelines. *See, e.g.*, 28 U.S.C. § 991(b), 994(b)(1), (h)-(l), (p).

Accordingly, both the Supreme Court and the Third Circuit have emphasized that "'a within-guidelines range sentence is *more likely* to be reasonable than one that lies outside the advisory guidelines range[.]'" *United States v. Goff*, 501 F.3d 250, 257 (3d Cir. 2007) (emphasis by Circuit); *Cooper*, 437 F.3d at 331-32. "[W]here judge and Commission both determine that the Guidelines sentences is an appropriate sentence for the case at hand, that sentence likely reflects the § 3553(a) factors (including its "not greater than necessary" requirement)," and that "significantly increases the likelihood that the sentence is a reasonable one." *Rita*, 127 S. Ct. at 2463, 2465, 2467.

E. Policy Statements

As set forth above, the advisory Guideline range is also supported by the "pertinent policy statements" in the Guidelines, 18 U.S.C. § 3553(a)(5), under which no departures are warranted.

IV. The Court Should Explain the Reasons for its Sentence

There must be "an explanation from the district court sufficient for [the Circuit] to see that the particular circumstances of the case have been given meaningful consideration within the parameters of § 3553(a)." *Levinson*, 543 F.3d at 196; *Goff*, 501 F.3d at 254, 256. The record must also disclose "the exercise of independent judgment, based on a weighing of the relevant factors, in arriving at a final sentence." *Grier*, 475 F.3d at 571-72. "A reasoned and rational justification for a sentence is necessary[.]" *Id.* at 572.

The Court must also "acknowledge and respond to any properly presented sentencing argument which has colorable legal merit and a factual basis." *Ausburn*, 502 F.3d at 329 & n.33; *United States v. Sevilla*, 541 F.3d 226, 232 (3d Cir. 2008); 18 U.S.C. § 3553(c). Even for lesser arguments, the Third Circuit has stated that "[e]xplicit rulings are plainly to be preferred, however, both for the benefit of the parties and for this court on review." *Goff*, 501 F.3d at 255-56 & n.10 (courts "should expressly deal with arguments emphasized by the parties").

Thus, the Court "'should set forth enough to satisfy the appellate court that [s]he has considered the parties' arguments and has a reasoned basis for exercising his own legal decisionmaking authority.'" *United States v. Lessner*, 498 F.3d 185, 203 (3d Cir. 2007); *Gall*, 128 S. Ct. at 597. "Merely reciting the § 3553(a) factors, saying that counsel's arguments have been considered, and then declaring a sentence, are insufficient[.]" *United States v. Jackson*, 467 F.3d 834, 841-42 (3d Cir. 2006).

V. Conclusion

Accordingly, Andrew Auernheimer should be sentenced to a term of imprisonment within the Guidelines range and three years of supervised release.

Thank you for your consideration.

Respectfully submitted,

PAUL J. FISHMAN
United States Attorney

/s/ Zach Intrater
By: Michael Martinez
Executive Assistant U.S. Attorney
Zach Intrater
Assistant U.S. Attorney

cc: Tor Ekeland, Esq. (via e-mail)
Mark Jaffe, Esq. (via e-mail)
Nace Naumoski, Esq. (via e-mail)
United States Probation Officer Joshua MacAvoy (via e-mail)